UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/399,192	09/17/1999	JOHN WANKMUELLER	AP31994-0704	1972

7590 02/26/2003

BAKER & BOTTS LLP
30 ROCKEFELLER PLAZA
NEW YORK, NY 101120228

EXAMINER
HUSEMAN, MARIANNE

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 02/26/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/399,192	WANKMUELLER ET AL.	
	Examiner	Art Unit	
	M. Huseman	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 October 2002* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 September 1999* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 10/22/02 have been fully considered but they are not persuasive. Applicants' state in their remarks that neither Fak et al, Konheim et al (hereinafter referred to as Fak and Konheim, respectively) nor Rosenow teach a second transaction type. However, the Examiner interprets the first transaction type as the card/PIN of Fak (or Konheim or Rosenow) being used as a credit card and the second transaction type as the card/PIN of Fak (or Konheim or Rosenow) being used as either a debit or credit card. The first set of identification data reads on the PIN (first transaction type equivalent to the present use of the card – credit or debit). A cryptographic operation is performed upon the first set of identification data thereby generating a second set of identification data (ciphers) which are used to validate the cardholder for any transaction presently desired by the cardholder (second transaction type equivalent to either an ATM transaction or purchase transaction). One card/PIN but two different transaction types are possible. Therefore, in addition to new drawing objections and 35 USC § 112 paragraph 1 and 2 rejections, the art rejections of the first office action stand and are repeated below.

Drawings

2. The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the system, including a memory and a processor, of claims 17 – 48 must be shown or the feature(s) canceled from the claim(s). Also, a block diagram illustrating the method claims is also required; i.e., a diagram showing "a first set of identification data" being inputted to a block that performs "a cryptographic operation upon the first set of identification data" and outputs (generates) "a second set of identification data" as is claimed in claims 1 – 13, 17 – 29, 33 – 45, 49 and 50. No new matter should be entered.

A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1 – 13, 17 – 29, 33 – 45, 49 and 50 are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. It is not clear from the specification as to what applicants mean by a "first transaction type" and a "second transaction type"; i.e., what type of transaction is related to the first set of identification data and what type of transaction is related to a second set of identification data? More explanation is needed in the specification if it is different from the teachings of, for example, Fak et al (or Konheim et al) and hence the interpretation of the Examiner. See also, paragraph 1, above.

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 41 – 43 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In claim 41, the phrase "A method according to..." should be changed to - -the system of claim 40- - to provide consistent claim language.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claim 1-5, 17-20, and 33-36 are rejected under 35 U.S.C. 102(b) as being anticipated by Fak et al.

Re claim 1: Fak (col. 2, lines 3-11) discloses a method for generating identification data, comprising the steps of:

providing a first set of identification data (i.e., an account number) related to a first transaction type; and

performing a cryptographic operation upon the first set of identification data (i.e., derived by generating a first cipher Y1 by encrypting the account number using the PIN in combination with a first secret security number as a key), thereby generating a second set of identification data (i.e., a check number) related to a second transaction type.

Re claim 2: Fak further discloses that the step of performing a cryptographic operation comprises:

providing a conversion key (i.e., a first cipher Y1); and

using the conversion key to perform said cryptographic operation upon the first set of identification data (i.e., derived by generating a first cipher Y1 by encrypting the account number using the PIN in combination with a first secret security number as a key).

Re claim 3: Fak further discloses that the step of providing a conversion key comprises: providing conversion key derivation data (i.e., PAN);

providing a conversion key derivation key (i.e., PIN or a first secret security number as a key); and

performing the cryptographic operation upon the conversion key derivation data and the conversion key derivation key (i.e., "by encrypting the PAN using the PIN in combination with a first secret security number as a key").

Re claim 4: Fak further discloses that the step of performing a cryptographic operation upon the conversion key derivation data and the conversion key derivation key comprises using the conversion key derivation key (i.e., PIN or a first secret security number as a key) to perform at least one cryptographic operation upon the conversion key derivation data (i.e., "by encrypting the PAN using the PIN in combination with a first secret security number as a key").

Re claim 5: Fak further discloses that the conversion key derivation data includes an identification number (i.e., "PAN") that is associated with multiple accounts (i.e., a bank card would inherently have multiple accounts such as saving and checking account), and wherein at least one cryptographic operation using a secret key (i.e., "a first secret security number as a key") is performed to cryptographically process said conversion key derivation data to produce the conversion key (i.e., "by encrypting the PAN using the PIN in combination with a first secret security number as a key").

Re claims 17-20 and 33-36: The claimed system would have been inherent to perform the method disclosed by Fak as stated above.

9. Claims 1, 6, 7, 12, 17, 22, 23, 28, 33, 38, 39 and 44 rejected under 35 U.S.C. 102(b) as being anticipated by Konheim et al.

Re claim 1: Konheim (FIG. 5A) discloses a method for generating identification data, comprising the steps of.

providing a first set of identification data (i.e., "M1") related to a first transaction type; and

performing a cryptographic operation upon the first set of identification data (i.e., "E(K, MI)", thereby generating a second set of identification data (i.e., "M2"').

Re claim 6: Konheim further discloses that the step of performing a cryptographic operation comprises:

providing cryptographically-computed data (i.e., "PINTRUE"); and

performing an operation upon the first set of identification data (i.e., "M1") and the cryptographically-computed data (i.e., "PINTRUE').

Re claim 7: Konheim further discloses that the step of providing cryptographically-computed data comprises:

providing initial data (e.g., "MI"); and

performing at least one cryptographic operation (i.e., "E(K,M1)") using a secret key (i.e., "K") upon the initial data (i.e., "M 1"), thereby producing the cryptographically-computed data (i.e., "PINTRUE").

Re claim 12: Konheim further discloses that the step of providing cryptographically computed data comprises generating a cryptographically-computed number having a base
corresponding to a base of a number representing the first set of identification data, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the first set of identification data (i.e., "PINTRUE = E(K,M1)").

Re claims 17, 22, 23, 28, 33, 38, 39, and 44: The claimed system would have been inherent to perform the method disclosed by Konheim as stated above.

10. Claims 14, 15, 30, 31, 46, 47, 49 and 50 are rejected under 35 U.S.C. 102(b) as being anticipated by Rosenow.

Re claim 14: Rosenow (e.g., col. 18, lines 26-40) discloses a method for generating a cryptography key, comprising:
providing a key derivation key (i.e., "Pin Verification Key");
using the key derivation key (i.e., "Pin Verification Key") in a cryptographic operation (i.e., "DES algorithm") performed on data obtained from an identification number (i.e., "the customer's Personal Account Number", thereby producing the cryptographic key (i.e., "the customer PIN").

Re claim 15: Rosenow further discloses the step of generating a key-check value suitable for determining whether data received corresponds to the cryptography key (col. 18, lines 36-40).

Re claims 30, 31, 46, and 47: The claimed system would have been inherent to perform the method disclosed by Rosenow as stated above.

Re claim 49: Rosenow discloses a method for generating identification data for an electronic financial transaction over a communications network, comprising the steps of providing a first set of identification data related to a first transaction type (e.g., col. 17, lines 1-3);
performing a cryptographic operation upon the first set of identification data to generate a second set of identification data for use in conducting said electronic financial transaction (e.g., col. 17, lines 3-6).

Re claim 50: Rosenow further discloses that the first set of identification data is an ATMPIN, said first transaction type is an ATM-transaction (e.g., col. I, lines 35-39; col. 17, lines 1-3), said second set of identification data is an electronic commerce PIN (e.g., encrypted PIN used for communicating financial transaction; col. 17, lines 3-9), said electronic financial transaction is an electronic commerce transaction, said method further comprising the step of

performing a second cryptographic operation upon said electronic commerce PIN to generate said ATM-PIN (e.g., decrypting the encrypted PIN; col. 17, lines 6-13).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 8 – 11, 13, 24 – 29, 40 – 43 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Konheim.

Re claim 8: Konheim does not explicitly disclose that the at least one cryptographic operation using a secret key comprises at least one of a DES-encryption and a DES-decryption. However, a DES-encryption and a DES-decryption are old and well known in the cryptographic art.

Re claim 9: Konheim further discloses that least a portion of the initial data is obtained from at least a portion of an account number (i.e., "M1 ").

Re claims 10 and 13: Konheim does not explicitly disclose that the operation upon the first set of identification data and the cryptographically-computed data comprises either a subtraction operation or an addition operation. However, the use of a subtraction operation or an addition operation is old and well known in the cryptographic art.

Re claim 11: Konheim further discloses that the step of providing cryptographicallycomputed data further comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the first set of identification data, wherein said cryptographically-computed number has a

number of digits corresponding to a number of digits of said number representing the first set of identification data (i.e., "PINTRUE = E(K,M1)").

Re claims 24-29, 40-43, and 45: The claimed system would have been obvious to perform the claimed method which would have been obvious in view of Konheim as stated above.

13. Claims 16, 32 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rosenow in view of Ford et al. (Ford hereinafter: "Secure Electronic Commerce", Prentice Hall
PTR, 1997).

Rosenow does not explicitly disclose the multiple encryption approach. However, Ford
discloses the multiple encryption approach to enhance the security of electronic commerce (page
104). Thus, it would have been within the level of ordinary skill in the art to modify the method
and system of Rosenow by adopting the teaching of Ford to enhance the security of electronic
commerce.

14. Claims 21 and 37 rejected under 35 U.S.C. 103(a) as being unpatentable over Fak in view of Ford.

Fak does not explicitly disclose the multiple encryption approach. However, Ford discloses the multiple encryption approach to enhance the security of electronic commerce (page
104). Thus, it would have been within the level of ordinary skill in the art to modify the system of
Fak by adopting the teaching of Ford to enhance the security of electronic commerce.

Conclusion

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to M. Huseman whose telephone number is 703-605-4277. The examiner can normally be reached on Monday - Friday, 6:30 AM - 3:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on 703-305-9768. The fax phone numbers for the organization where this application or proceeding is assigned are 703-305-7687 for regular communications and 703-305-7687 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-1113.

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

M. Huseman

M. Huseman
Examiner
Art Unit 3621

mh
February 24, 2003